УДК 004.056.53

**М. С. Иванов**
Научный руководитель: д-р тех. наук, проф. А. А. Захаров
Тюменский государственный университет, Тюмень

# ИСПОЛЬЗОВАНИЕ NFC ТЕЛЕФОНА С ОПЕРАЦИОННОЙ СИСТЕМОЙ ANDROID КАК ВТОРОГО ФАКТОРА АУТЕНТИФИКАЦИИ

*Аннотация*. В данной работе было разработано программное средство для Android, реализующее стандарт U2F и позволяющие с помощью электронной подписи использовать телефон с модулем NFC как дополнительный фактор аутентификации. В работе ставилась проблема удобства и безопасности использования различных видов двухфакторной аутентификации. Целью работы является исследование возможности использования телефона с NFC как одного из факторов аутентификации и разработка программного обеспечения для безопасной аутентификации пользователя при помощи NFC.

*Ключевые слова:* компьютерная безопасность; аутентификация; NFC; двухфакторная аутентификация; Android; U2F.

В настоящее время уже недостаточно использования фактора знания логина и пароля пользователем для надежной аутентификации в сервисах, особенно в сервисах с важными активами, таких как дистанционное банковское обслуживание, медицина, управление финансами, вход в аккаунт почты или просто вход в корпоративный ПК. Для улучшения безопасности существует множество вариантов использования многофакторной аутентификации для удаленных сервисов: SMS, TOTP, HOTP, USB или цифровые токены. Но данные методы или не предоставляют требуемой степени безопасности или неудобны в применении. Поэтому был разработан способ аутентификации с помощью NFC телефона с возможностью производить аутентификацию в одно касание к считывателю.

Во многих современных телефонах присутствует NFC-модуль, позволяющий работать в трех режимах: считывания и записи меток; режим p2p; режим эмуляции бесконтактной банковской карты. В работе используется режим эмуляции карты, который предоставляет возможность обмениваться APDU сообщениями со считывателем [1].

U2F — это стандарт, выпущенный консорциумом FIDO Alliance для быстрой, удобной и безопасной двухфакторной аутентификации с помощью отдельного устройства [2]. Данный вид аутентификации предполагает наличие у пользователя отдельного фактора владения криптоключом. Протокол U2F

использует принцип посылки сервисом уникального challenge и ответа клиента с подписью, использующим алгоритм ECDSA с эллиптической кривой secp256r1. Протокол аутентификации в этой работе основан на данном стандарте.

Основной функционал программы работает в режиме Host-based Card Emulation сервиса Android. Данный сервис был зарегистрирован с APDU SELECT AID равным A0000006472F0001. Таким образом, он отвечает на NFC сообщения от считывателей, делающих запросы на регистрацию или аутентификацию.

Программа реализует две основные функции: регистрация и аутентификация.

Во время регистрации сервер посылает клиенту через посредника сообщение, содержащие appId (идентификатор сервиса), challenge (уникальное задание для подписи клиентом). Посредник преобразует сообщение в бинарный формат и передает через необходимый канал передачи, такой как USB-HID, Bluetooth, NFC на криптографический токен, или клиент. Клиент генерирует приватный ключ для эллиптической кривой NIST P-256 или имеющей другое название secp256r1. Устройство аутентификации подписывает ответное сообщение с помощью своего сертификата и передает проверяющей стороне.

Далее от данного сервиса уже пойдут сообщения с командой аутентификации клиента. Так, сервер аутентификации посылает клиенту задание со следующим набором полей: appId (идентификатор сервиса), challenge (уникальное задание для подписи клиентом), keyHandle (идентификатор ключа клиента). Клиент при нахождении ключа для данных appId и keyHandle отвечает подписью входящего запроса и счетчиком подписей, который служит для обнаружения клонирования клиента аутентификации. После этого сервер проверяет подпись клиента с открытым ключом из базы данных.

Таким образом, с помощью описанных выше процедур, данное приложение уже можно использовать для безопасной аутентификации пользователя на различных сервисах, поддерживающих U2F, и с наличием NFC-считывателя.

**Список литературы**

1. *Рабинович А. С.*, *Казарин О. В.* Методика аутентификации пользователя в информационной системе с использованием технологии NFC [Электронный ресурс] // Вопр. кибербезопасности. 2013. № 2. URL: http://cyberleninka.ru/article/n/metodika-autentifikatsii-polzovatelya-v-informatsionnoy-sisteme-s-ispolzovaniem-tehnologii-nfc (дата обращения: 01.11.2017).

2. FIDO NFC Protocol Specification v1.0 [Электронный ресурс] // 11.04.2017 URL: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-nfc-protocol-v1.2-ps-20170411.pdf (дата обращения: 02.11.2017).